REMARKS

Applicant respectfully requests reconsideration and allowance in view of the following remarks. Claims 1-7 are pending in the application.

Section 102 Rejections:

In the Office Action, claims 1-7 were rejected under 35 U.S.C. 102(e) as being anticipated by Kocher (US Patent No. 6,327,661).

With regard to independent claim 1, Applicant notes that this claim recites that during encryption of the digital data, a data bit word generated on the basis of random numbers is stored in a storage cell (10) before a data word is written therein such that the storage cell (10) is pre-initialized with random data. In contrast, Kocher generally describes a noise production module 105 that "is configured to sink power, produce electromagnetic radiation, or otherwise introduce noise into attackers' measurements, where the noise produced is a function of [an analog] input." Col. 5, lines 25-30. This analog input is generated either directly by an analog randomness source 101, or by using a noise processing module 102 to process random digital data and a D/A converter 104 to convert the processed data to analog form. Col. 5, lines 38-41; Col. 4, lines 63-67; Col. 5, lines 23-25. Applicant, accordingly, respectfully submits that Kocher generally describes generating random data that is used in analog form to sink power or produce electromagnetic radiation, not storing in a storage cell a data bit word generated on the basis of random numbers before a data word is written therein such that the storage cell is pre-initialized with random data as recited in claim 1.

Furthermore, even assuming *arguendo* that the random data generated by Kocher is stored in a storage cell, the storage cell is not the same as the storage cell used to store data words on which cryptographic sub-operations are performed as also required by claim 1. Although the noise production system 100 is activated during periods in which encryption is performed, the data generated by the noise production system 100 is used independently of the data used by the cryptographic system. Col. 5, lines 44-60. Embodiments of claim 1 provide significant advantages over Kocher by pre-initializing storage cells with random data so as to prevent information concerning the data words written into the storage cell from being extracted on the basis of variations in the current consumption during the writing into the storage cells. Therefore, because Kocher fails to teach or suggest claim 1, Applicant respectfully requests that the Section 102(e) rejections with respect to claim 1 and all claims dependent thereon be withdrawn.

In view of the foregoing remarks, Applicant respectfully submits that claims 1-7 are in condition for allowance. Applicant, accordingly, respectfully requests that a notice of allowance be issued with respect to claims 1-7.

Please charge any fees which may be required, except the issue fee, or credit any overpayment to Deposit Account No. 14-1270.

Date: May 19, 2004

Respectfully submitted,

By _____

Kevin Simons, Reg. No. 45,110
(408) 474-9075
Philips Electronics North America
1109 McKay Drive; Mail Stop SJ41
San Jose, CA 95131 USA